

Databehandlersaftale

mellem

Parterne

København Øjen & Skeleklunik

Jægersborgvej 66A, 2. th

2800 Kgs. Lyngby

CVR-nr. 31569281

(Herefter kaldt den **Dataansvarlige**)

Og

Region Nordjylland som Fælles Systemadministrator

Niels Bohrs Vej 30

9220 Aalborg Øst

CVR-nr. 29 19 09 41

(Herefter kaldt **Databehandleren**)

Er der indgået nedenstående databehandlersaftale (herefter **Databehandlersaftalen**) om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige.

1. Definitioner

Dataansvarlig	En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den Dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret.
Databehandler	En fysisk eller juridisk person, en offentlig myndighed, en institution eller andet organ, der behandler personoplysninger på den Dataansvarliges vegne.
Hovedaftale	Den aftale eller kontrakt, der er indgået mellem parterne vedrørende udførelse af de opgaver, hvortil Databehandleraftalen er knyttet.
Sikkerhedsgodkendelse	Ved sikkerhedsgodkendelse forstås en status, som en person tildeles efter en personundersøgelse, således at denne kan få adgang til klassificeret materiale eller -områder. I Danmark foretages personundersøgelser og sikkerhedsgodkendelser af Politiets Efterretningstjeneste.
Tredjelande og internationale organisationer	Et tredjeland er et land, som ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge). En international organisation kan f.eks. være Røde Kors, WHO, FN, OECD m.fl. For at reglerne i forordningens kapitel V finder anvendelse på internationale organisationer, er det en forudsætning, at den internationale organisation befinder sig i et tredjeland.
Underdatabehandler	En Databehandler, som Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige.

2. Generelt

- 2.1 Denne databehandlersaftale vedrører den Dataansvarliges og Databehandlerens forpligtelse til at efterleve EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om ophævelse af direktiv 95/46EF (generel forordning om databeskyttelse) samt lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).
- 2.2 Principperne og anbefalingerne i ISO27001 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang, andet ikke fremgår af nærværende Databehandlersaftale.
- 2.3 Databehandleren skal behandle personoplysninger i overensstemmelse med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
- 2.4 Er det i forbindelse med indgåelsen af nærværende Databehandlersaftale aftalt, at Databehandleren forpligter sig til at gøre sig bekendt med og efterleve den Dataansvarliges informationssikkerhedspolitik eller andre sikkerhedsretningslinjer, skal dette fremgå af punkt 17.2.
- 2.5 Databehandlersaftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

3. Formål

- 3.1 Databehandlerens opgave og formålet med databehandlingen fremgår af punkt 17.1.
- 3.2 Databehandleren må ikke behandle oplysninger omfattet af denne Databehandlersaftale til egne formål.

4. Den Dataansvarliges rettigheder og forpligtelser

- 4.1 Den Dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

- 4.2 Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
- 4.3 Den Dataansvarlige er blandet andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

5. Databehandlerens generelle forpligtelser

- 5.1 Databehandleren er Databehandler for de personoplysninger, som behandles på vegne af den Dataansvarlige iht. Hovedaftalen og Databehandleraftalen.
- 5.2 Databehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige og alene i det omfang, det er nødvendigt for, at Databehandleren kan opfylde sine forpligtelser iht. Hovedaftalen og Databehandleraftalen. jf. bilag 1 Databehandlerinstruks, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, jf. punkt 10.1.
- 5.3 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med Databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.
- 5.4 Databehandleren har de forpligtelser, som er pålagt Databehandleren i medfør af lovgivningen, jf. punkt. 2.1.
- 5.5 Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor den Dataansvarliges personoplysninger opbevares, jf. punkt 17.1. Databehandleren skal underrette den Dataansvarlige om enhver ændring.
- 5.6 Denne databehandleraftale frigør ikke Databehandleren for de forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt Databehandleren.

6. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 6.1 Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

- 6.2 Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
- a. Pseudonymisering og kryptering af personoplysninger
 - b. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester
 - c. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - d. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed
- 6.3 Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag 1.
- 6.4 Databehandleren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandling af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed iagttages.
- 6.5 Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den Dataansvarliges personoplysninger, om Databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. punkt 11 samt bilag 1 Databehandlerinstruks.

7. Anvendelse af ad hoc arbejdspladser

- 7.1 Anvendelse af ad hoc arbejdspladser (fjern- eller hjemmearbejdspladser) skal være godkendt af den Dataansvarlige.
- 7.2 Såfremt Databehandleren foretager databehandling fra ad hoc arbejdspladser, skal Databehandleren sikre, at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag samt Datatilsynets IT-sikkerhedstekster herom.
- 7.2.1 I det omfang databehandlingen sker fra ad hoc arbejdspladser, skal Databehandleren i punkt 17.2 beskrive
- Hvilken krypteret forbindelse, der anvendes mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk
 - Anvendelse af 2-faktor-autentifikation
 - Databehandlerens instruks til egne medarbejdere om anvendelse af ad hoc arbejdspladser.

8. Underretningspligt og assistance

- 8.1 Databehandleren forpligter sig til uden unødigt forsinkelse og skriftligt, at orientere den Dataansvarlige om afvigelser fra kravene i databehandleraftalen, f.eks.:
- Ved enhver fravigelse fra givne instrukser
 - Ved enhver afvigelse fra det aftalte om tilgængelighed
 - Ved planlagte releases, opgraderinger, tests mv.
 - Ved enhver mistanke om brud på fortroligheden, misbrug, fortabelse og forringelse af data mv.
- 8.2 Yderligere forpligter Databehandleren sig til uden unødigt forsinkelse og senest 24 timer efter, at denne er blevet bekendt med bruddet skriftligt at orientere den Dataansvarlige om brud på persondatasikkerheden, f.eks.:
- Ved enhver konstatering af misbrug, tab og forringelse af data mv.
 - Ved enhver hændelig eller uautoriseret videregivelse af eller adgang til personoplysningerne behandlet efter denne databehandleraftale

Sådan at den Dataansvarlige har mulighed for at efterleve forpligtelsen til at anmelde bruddet til tilsynsmyndigheden inden for 72 timer

En underretning om brud på persondatasikkerheden skal indeholde følgende oplysninger:

- karakteren af bruddet på datasikkerheden og, hvis det er muligt, hvem der er omfattet, antal berørte og antal berørte registreringer af personoplysninger
 - beskrivelse af de sandsynlige konsekvenser der er af bruddet
 - beskrivelse af de foranstaltninger databehandleren har truffet eller foreslår truffet for at håndtere databruddet og hvad der kan gøres for at begrænse dets mulige skadevirkninger
- 8.3 Databehandleren skal følge op på sikkerhedshændelsen og underrette den Dataansvarlige om de nærmere omstændigheder, herunder udarbejde en situationsrapport samt oplyse om, hvilke personoplysninger, der er kompromitteret, samt hvilke tiltag Databehandleren har iværksat eller påtænker at iværksætte.
- 8.4 Databehandleren og dennes underdatabehandlere må hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud uden forudgående skriftlig aftale med den Dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren er retligt forpligtet til sådan kommunikation.
- 8.5 Databehandleren og dennes eventuelle Underdatabehandlere skal uden unødigt forsinkelse bistå den Dataansvarlige med håndteringen af enhver henvendelse fra en registreret, herunder anmodning om indsigt, berigtigelse, blokering eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Databehandleren og dennes eventuelle Underdatabehandlere skal ligeledes bistå den Dataansvarlige med at overholde øvrige

forpligtelser, der måtte påhvile den Dataansvarlige efter gældende ret, hvor bistanden er forudsat, samt bistand er nødvendigt for, at den Dataansvarlige kan overholde sine forpligtelser.

9. Databehandlerens brug af Underdatabehandler¹

- 9.1 Databehandleren må ikke uden udtrykkelig skriftligt samtykke fra den Dataansvarlige anvende andre underdatabehandlere end dem, der er angivet i bilag 2, til at behandle personoplysninger, som den Dataansvarlige har overladt til Databehandleren i medfør af databehandleraftalen og Hovedaftalen. Den Dataansvarlige er berettiget til at stille vilkår for et sådant samtykke.
- 9.2 Databehandleren skal indgå en skriftlig aftale med sin underdatabehandler, hvor det sikres, at underdatabehandleren som minimum kan opfylde de forpligtelser, som Databehandleren har påtaget sig ved denne Databehandleraftale, for så vidt angår den behandling af personoplysninger, der varetages af underdatabehandleren. Databehandleren indestår for kontraktmæssigheden og lovligheden af underdatabehandlerens behandling af personoplysninger. Det forhold, at databehandleren indgår aftale med en underdatabehandler, fritager ikke Databehandleren for pligten til at efterleve nærværende Databehandleraftale.
- 9.3 Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den Dataansvarlige.
- 9.4 Det er Databehandlerens ansvar at sikre og dokumentere, at eventuelle underdatabehandlere, er bekendt med og efterlever den Dataansvarliges instruks (bilag 1).
- 9.5 Al kommunikation mellem den Dataansvarlige og underdatabehandleren skal som udgangspunkt ske via Databehandleren.
- 9.6 Ved ophør af en aftale med en underdatabehandler skal Databehandleren give den Dataansvarlige meddelelse herom. Databehandleren skal i den forbindelse sikre, at underdatabehandleren sletter data behørigt i overensstemmelse med kravene i punkt 13.

Skift af underdatabehandler i aftaleperioden

- 9.7 Databehandleren kan udpege en ny Underdatabehandler, såfremt den nye Underdatabehandler (1) overholder gældende love om databeskyttelse og (2) er bundet af en databehandleraftale og (3) har et sikkerhedsniveau som er mindst den samme som den nuværende Underdatabehandler.

¹ Såfremt underdatabehandleren er etableret i et tredjeland, skal reglerne i kapitel 11 ligeledes iagttages.

- 9.8 Databehandleren skal orientere den Dataansvarlige i tilfælde af, at der vælges en ny Underdatabehandler. Orienteringen skal ske senest 3 måneder inden den nye Underdatabehandler tages i anvendelse.
- 9.9 Såfremt den Dataansvarlige ikke mener, at en af Databehandleren udpeget Underdatabehandler lever op til et eller flere af de ovennævnte krav under punkt (1), (2) og (3), vil det blive betragtet som væsentlig misligholdelse og der henvises til punkt 14 om misligholdelse. Inden væsentlig misligholdelse gøres gældende skal den Dataansvarlige underrette sin Databehandler om forholdet og give en passende frist til at udbedre misligholdelsen.

10. Overførsel af personoplysninger til tredjelande eller internationale organisationer

- 10.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. databeskyttelsesforordningens art. § 28, stk. 3, litra a.
- 10.2 Uden den Dataansvarlige instruks eller godkendelse kan Databehandleren – indenfor rammerne af Databehandleraftale – derfor bl.a. ikke;
- a) videregive personoplysninger til en Dataansvarlige i et tredjeland eller i en international organisation,
 - b) overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland²,
 - c) lade oplysningerne behandle i en anden af Databehandlerens afdelinger, som er placeret i et tredjeland.
- 10.3 Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af dennes aftales punkt 17.2.

11. Tavshedspligt og fortrolighed

² Se også pkt. 9

- 11.1 Personoplysninger omfattet af denne aftale er fortrolige.
- 11.2 Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
- 11.3 Det påhviler Databehandleren og dennes eventuelle underdatabehandlere at informere egne ansatte, samarbejdspartnere, eksterne konsulenter, vikarer m.fl. om udstrækningen af tavshedspligten og om konsekvenserne ved en eventuel overtrædelse.
- 11.4 Kun de personer hos Databehandleren eller dennes underdatabehandlere, der autoriseres hertil, må have adgang til de personoplysninger, der behandles og brugerne må kun autoriseres til anvendelser, de har behov for i forhold til at kunne opfylde Databehandlerens forpligtelser over for den Dataansvarlige.
- 11.5 Databehandleren og dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 11.6 Databehandlerens forpligtelser om tavshedspligt og fortrolighed gælder også efter aftalens ophør.

12. Audit og revisionserklæringer

- 12.1 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige de nødvendige oplysninger til, at denne kan påse forpligtelserne i henhold til denne aftale samt at der er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger. Endvidere skal Databehandleren kunne dokumentere, at identificerede sårbarheder bliver imødegået ud fra en risikobaseret vurdering.
- 12.2 Såfremt den Dataansvarlige, en repræsentant for den Dataansvarlige, dennes revision (intern eller ekstern) eller en relevant offentlig myndighed, særligt Datatilsynet, ønsker at foretage fysisk inspektion (audit) af de foranstaltninger, som Databehandleren har etableret i medfør af aftalen, forpligter Databehandleren sig til - med et rimeligt varsel - at stille tid og ressourcer til rådighed herfor. Databehandleren forpligter sig til på samme måde at sikre, at sådanne audits kan gennemføres hos sine eventuelle underdatabehandlere.
- 12.3 Som supplement eller alternativ til de overfor nævnte audits kan der indgås aftale om, at Databehandleren og eventuelle underdatabehandlere for egen regning sørger for, at en uafhængig ekspert årligt udarbejder en revisionserklæring på grundlag af en anerkendt standard angående Databehandlerens overholdelse af kravene til sikkerhedsforanstaltninger fastsat i Databehandleraftalen. Erklæringen skal være formuleret konkret i forhold til den opgave, som Databehandleren løser for den Dataansvarlige. En sådan aftale skal fremgå af punkt 17.2.

13. Håndtering af data efter aftalens ophør

- 13.1 Databehandleren og dennes eventuelle underdatabehandlere forpligter sig til at tilbagelevere og/eller slette personoplysninger, når databehandlingen i henhold til Hovedaftalen med den Dataansvarlige ophører medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.
- 13.2 Den Dataansvarlige skal inden Hovedaftalens ophør skriftligt meddele Databehandleren, hvorvidt alle personoplysninger skal slettes eller tilbageleveres til den Dataansvarlige. Fristen herfor aftales mellem parterne.
- 13.3 Databehandleren er ansvarlig for, at sletning af oplysningerne sker på en sådan måde, at det ikke er muligt at genskabe oplysningerne. Databehandleren er herunder ansvarlig for at oplysningerne også slettes fra backup samt hos eventuelle underdatabehandlere.
- 13.4 Hvis oplysningerne tilbageleveres til den Dataansvarlige, skal Databehandleren slette eventuelle kopier af oplysningerne.
- 13.5 Når sletningen er gennemført, skal Databehandleren fremsende en skriftlig erklæring på, at data er slettet som aftalt.
- 13.6 Såfremt Databehandleren eller dennes underdatabehandlere i forbindelse med konkurs eller lignende ophører med at behandle personoplysninger for den Dataansvarlige, skal alle personoplysninger uden ugrundet ophold tilbageleveres på en måde, der gør det muligt for den Dataansvarlige at anvende disse fremadrettet. Databehandler, dennes konkursbo e.l. er herefter forpligtet til at slette oplysninger fra deres egne systemer i overensstemmelse med pkt. 13.1-13.5.

14. Misligholdelse

- 14.1 Bestemmelserne i dette afsnit har forrang ift. Hovedaftalen, for så vidt angår behandlingen af personoplysninger. Såfremt dette ikke er tilfældet, angives det i pkt. 17.1.
- 14.2 Ved Databehandlerens misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at gøre sædvanlige misligholdelsesbeføjelser gældende med de tilføjelser og præciseringer, som fremgår af bestemmelserne i dette afsnit.
- 14.3 Ved væsentlig misligholdelse af Databehandleraftalen er den Dataansvarlige berettiget til at ophæve Hovedaftalen og dermed også Databehandleraftalen. Som udgangspunkt betragtes det som væsentlig misligholdelse, såfremt Databehandleren ikke overholder forpligtelserne i

Databehandleraftalen, den til enhver tid gældende lovgivning vedrørende databeskyttelse samt kravene i de dokumenter, der udgør bilag til Databehandleraftalen.

- 14.4 Den Dataansvarliges ophævelse af Hovedaftalen og Databehandleraftalen indebærer ikke, at den Dataansvarlige giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt, jf. pkt. 14.7.
- 14.5 Såfremt den Dataansvarlige vælger ikke at ophæve Hovedaftalen og Databehandleraftalen i ét eller flere tilfælde, selvom den Dataansvarlige er berettiget hertil, medfører dette ikke, at den Dataansvarlige mister retten til at ophæve Hovedaftalen og Databehandleraftalen i andre tilfælde.
- 14.6 Ved ophævelse af Hovedaftalen og Databehandleraftalen, er Databehandleren forpligtet til at levere databehandling i henhold til Hovedaftalen og denne Databehandleraftale, indtil databehandlingen er sikret hos en anden databehandler. Databehandleren er ligeledes forpligtet til at levere relevant ophørsassistance til den Dataansvarlige, herunder i relation til eventuelle underdatabehandlere, som Databehandleren måtte have overladt en del af databehandlingen til.
- 14.7 Databehandleren er erstatningsansvarlig i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af Databehandleraftalen. Såfremt den Dataansvarlige af tredjemand gøres erstatningsansvarlig for Databehandlerens og/eller eventuelle Underdatabehandleres manglende overholdelse af Databehandleraftalen, herunder Databehandleraftalens bilag, og/eller overtrædelse af gældende lovgivning vedrørende databeskyttelse, skal Databehandleren holde den Dataansvarlige skadesløs for alle omkostninger, gebyrer, erstatningsbeløb, udgifter eller tab, som den Dataansvarlige har afholdt eller pådraget sig som følge heraf.
- 14.8 Den Dataansvarlige er berettiget til at stille krav om, at Databehandleren bistår med at forsvare den Dataansvarliges interesser i en eventuel rets- eller voldgiftssag, uagtet Databehandlerens eventuelle indsigelser i forhold til den påberåbte misligholdelse, såfremt Databehandlerens bistand er af væsentlig betydning for varetagelsen af den Dataansvarliges interesser.

15. Lovvalg og værneting

- 15.1 Medmindre lovvalg og værneting er direkte reguleret i Hovedaftalen, finder følgende bestemmelser anvendelse:
- 15.1.1 Denne Databehandleraftale inklusiv ethvert spørgsmål om Databehandleraftalens gyldighed er undergivet dansk ret.
- 15.1.2 Såfremt der opstår uoverensstemmelser mellem Parterne i forbindelse med

Databehandleraftalen, skal Parterne med en positiv, samarbejdende og ansvarlig holdning søge at indlede forhandlinger med henblik på at løse tvisten.

- 15.1.3 Hvis enighed ikke kan opnås via forhandling eller på anden vis, skal tvisten løses ved de danske domstole ved den Dataansvarliges hjemting.

16. Ikrafttræden og varighed

- 16.1 Nærværende Databehandleraftale indgås ved begge parters underskrift og gælder indtil behandlingen af personoplysninger i henhold til Hovedaftalen er ophørt og Databehandleren har slettet data, jf. pkt. 13.
- 16.2 Den Dataansvarlige og Databehandleren er solidariske ansvarlige for at sikre, at der foretages de nødvendige opdateringer i databehandleraftalen ved lovændringer, hvis den dataansvarlige forpligtes til at efterkomme nye sikkerhedsstandarder eller hvis der sker ændringer af tekniske eller organisatoriske forhold hos den Dataansvarlige og/eller Databehandleren

17. Specifikke forhold vedr. databehandlingen

(Såfremt Databehandlerens opgave, jf. Hovedaftalen, vedrører flere forskellige databehandlinger, er der angivet kopier af nedenstående tabeller til venstre i pdf-vinduet. Disse anvendes for hver enkelt databehandling, som Databehandleraftalen omfatter)

17.1 Generelle forhold

Databehandlingens navn	Behandling af privathospitalers oplysninger fra lokale patientjournaler til fremvisning i sundhedsjournalen på sundhed.dk
ID i den Dataansvarliges fortegnelse over databehandlinger	
ID i Databehandlerens fortegnelse	RN-2020-DB007 (2020-005218-9)
Hovedaftale/kontrakt (dato for indgåelse, journal-ID)	Beslutning truffet af Den Nationale Bestyrelse på møde den 29. september 2018 i forbindelse med Sundhedsjournal 3.0-projektet.
Databehandlingens formål	<p>Databehandleren modtager oplysninger fra den dataansvarliges patientjournal-system og søger for, at disse oplysninger udstilles i sundhedsjournalen på Sundhed.dk</p> <p>Databehandleren er ansvarlig for drift af e-journaldatabasen og e-journalapplikationen. Databehandleren indgår databehandleraftaler med eventuelle underdatabehandlere på vegne af den dataansvarlige.</p>
Generel beskrivelse af behandlingen	<p>Databehandleren modtager oplysninger fra den dataansvarliges patientjournal-system og udstiller disse oplysninger i sundhedsjournalen på Sundhed.dk.</p> <p>Databehandleren sørger for, at oplysningerne har det rette format til udstilling i sundhedsjournalen.</p> <p>Databehandleren sørger for afhjælpning af tekniske problemer og fejl – eventuelt ved kontakt til den dataansvarliges systemleverandør.</p>
Registrerede personer (kategorier af personer, der indgår i databehandlingen)	Borgere om hvem, der er registreret oplysninger i de lokale epj-systemer, der afgiver oplysninger til e-journaldatabasen.

Kategorier af personoplysninger	Almindelige personoplysninger, fx identifikationsoplysninger. Fortrolige oplysninger, fx cpr-nr. Følsomme personoplysninger, fx helbredsoplysninger i form af eksempelvis cave, diagnose, procedurer, behandling mv.
Evt. modtagere af oplysninger	Borgerne har adgang til egne oplysninger. Befuldmægtigede har adgang til borgeres oplysninger, såfremt der foreligger en fuldmagt. Sundhedsfaglige brugere har adgang til oplysninger om borgere, som de har i behandling.
Sletningsfrister	Oplysningerne slettes efter anvisning fra den dataansvarlige.
Evt. lov/bestemmelse, der hjemler databehandlingen	Sundhedsloven (lbk. nr. 903 af 26. august 2019 med senere ændringer) - særligt kap. 8 og 9.
Databehandlerens opgave	Databehandleren modtager oplysninger fra den dataansvarliges patientjournal-system og udstiller disse oplysninger i sundhedsjournalen på Sundhed.dk. Databehandleren sørger for, at oplysningerne har det rette format til udstilling i sundhedsjournalen. Databehandleren sørger for afhjælpning af tekniske problemer og fejl – eventuelt ved kontakt til den dataansvarliges systemleverandør.
Lokationer for databehandlingen	Region Nordjylland Niels Bohrs Vej 30 · 9220 Aalborg Øst Datacentre placeret på følgende adresser: Hadsundvej 190 9000 Aalborg Og Hobrovej 42 9000 Aalborg

17.2 Særlige forhold vedr. databehandlingen (hvis ikke relevant, markeres dette)

Evt. andre lovkrav, som databehandlingen er underlagt (f.eks. krav om, at data skal opbevares i Danmark eller evt. specifikke samtykkekrav)	Databehandlingen er ikke underlagt andre lovkrav.
Evt. andre krav, som den dataansvarlige pålægger databehandleren	Databehandleren skal overholde bilag 1 "Databehandlerinstruks". Bopælsregionen varetager henvendelser fra borgere vedr. privatmarkering af journaloplysninger. Databehandleren kan i forbindelse med tekniske problemer tage kontakt til den dataansvarliges systemleverandør. Kontaktoplysninger på systemleverandør udfyldes nedenfor.
Aftale mellem parterne om helt eller delvist fravigelse af krav i databehandleraftalen (Beskriv aftalte fravigelser og eventuelle kompenserende sikkerhedsforanstaltninger)	Håndteringen af de registreredes rettigheder varetages af den dataansvarlige. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.
Databehandleren forpligter sig til at efterleve den dataansvarliges informationssikkerhedspolitik og/eller retningslinjer. (Angiv relevante dokumenter)	
Den dataansvarlige har givet instruks om eller godkendelse af overførsel af personoplysninger til tredjeland eller international organisation (anfør også overførselsgrundlag efter databeskyttelsesforordningens kapitel 5).	Databehandleren må ikke uden den dataansvarliges godkendelse overføre personoplysninger til tredjelande eller internationale organisationer.

Særlige tekniske eller organisatoriske sikkerhedsforanstaltninger, som skal etableres hos Databehandleren (f.eks. sikkerhedsgodkendelse af medarbejdere)	Der stilles ikke krav om, at medarbejdere hos databehandleren skal sikkerhedsgodkendes.
Beskrivelse af sikkerhedsforanstaltninger ved anvendelse af ad hoc arbejdspladser efter aftale med den Dataansvarlige	Databehandleren skal blandt andet opfylde og dokumentere følgende: <ul style="list-style-type: none"> • Beskrivelse af anvendt krypteret forbindelse mellem ad hoc arbejdspladser og Databehandlerens netværk. • Anvendelse af 2-faktor-autentifikation. • Databehandlerens interne instruks til egne medarbejdere vedrørende ad hoc arbejdspladser.
Beskrivelse af sikkerhedsforanstaltninger ved eksterne kommunikationsforbindelser	Databehandleren modtager oplysninger fra den dataansvarlige via en SFTP-server, som tilgås via Sundhedsdatanettet. Underdatabehandleres adgang til oplysninger i e-journaldatabasen sker via VPN-forbindelse.
Uddybende beskrivelse af foranstaltninger til beskyttelse af transmission af personoplysninger over åbne netværk	Der må ikke transmitteres personoplysninger over åbne netværk uden stærk kryptering.
Opbevaringstid for log (hvis længere end 6 måneder, jf. punkt 5.2 i databehandlerinstruksen).	Logoplysninger opbevares i fem år.
Evt. aftale om udarbejdelse af revisionserklæring, herunder angivelse af type	

17.3 Kontaktoplysninger i forbindelse med underretning om sikkerhedshændelser

Kontaktpersoner hos den dataansvarlige ved almindelige afvigelser fra normal drift	
Funktion	Chef + tjener
Navn	Helena Buch Hesgaard
E-mail	HBH@ADLNET.DK + eyedoc@kbhskolen.dk

Telefon	61777793
Bemærkninger	
Kontaktpersoner hos den dataansvarlige ved kritiske fejl og sårbarheder samt ved mistanke herom	
Funktion	chf og øjenlæge
Navn	Helena Buch Hesgaard
E-mail	HBH@DAOLNET.dk + eyedoc@kblhskolen.dk
Telefon	61777793
Bemærkninger	
Kontaktpersoner hos den dataansvarliges systemleverandør (Novax !)	
Leverandør (firma)	Novax A/S
Funktion	DPO
Navn	Kim Hørby Fredborg
E-mail	KHFR@NOVAX.DK
Telefon	92154123
Bemærkninger	Ved fravær: Michael Munk Jacobsen 23261629/mmj@novax
Kontaktpersoner hos databehandleren ved almindelige afvigelser fra normal drift	
Funktion	SPOC Servicedesk Region Nordjylland
Navn	Support
E-mail	itsupport@rn.dk
Telefon	97649000
Bemærkninger	24/7 vagt
Kontaktpersoner hos databehandleren ved kritiske fejl og sårbarheder samt ved mistanke herom	
Funktion	Fællesregional systemadministrator
Navn	Helle Hesthaven
E-mail	Hebeh@rn.dk
Telefon	41180431
Bemærkninger	Ved fravær Chefvagt tlf: 72137599

18. Bilagsliste

Bilag 1 Databehandlerinstruks

Bilag 2 Underdatabehandler

For den Dataansvarlige

Dato: 10/9 2021

Navn: Helena Buch Hesgaard



Øjenlæge, PhD, FEBO
Helena Buch Hesgaard

Ydernr. 090247

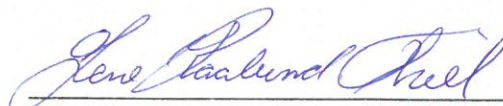
Jægersborgvej 66A, 2.th.
2800 Kgs. Lyngby

Tlf. 39 64 10 66

For Databehandleren

Dato: 17/9-2021

Navn: LONE KAPLUND THIEL



Underdatabehandler til databehandleren

Bilag 2

Databehandleren anvender følgende underdatabehandler(e) i forbindelse med de opgaver, som databehandleren udfører på vegne af den dataansvarlige.

Underdatabehandler	
Virksomhedens navn	Netcompany
Adresse	Grønningen 17, 1270 København K
Land	Danmark
CVR-nummer	39488914
Ansvarlig hos underdatabehandler	Team Manager Kristian Alban kral@netcompany.com 26112112
Kontaktperson hos underdatabehandler	Senior Developer Kenneth Raunkilde Ker@netcompany.com 22720236
Databehandling(er), som underdatabehandler deltager i	Databehandleren er ansvarlig for vedligeholdelse og videreudvikling af e-journal databasen og e-journal administrationsmodulet, hvorfra der kan udføres privatmarkering og organisationsspærringer. Derudover kan der via administrationsmodulet gives adgang til Forløbsoversigten, et overblik over udsendte Borgerbreve, Rapportering/statistik, Logning og fejl i dataleverancen.
Kategorier af data, som underdatabehandler behandler	Almindelige personoplysninger, fx identifikationsoplysninger. Fortrolige oplysninger, fx cpr-nr. Følsomme personoplysninger, fx helbredsoplysninger i form af eksempelvis diagnose, behandling mv.

Underdatabehandleren skal sikre, at kun medarbejdere, som er autoriseret til at arbejde med personoplysninger, må arbejde med den dataansvarliges personoplysninger. Underdatabehandler skal på efterspørgsel kunne fremvise skriftlig autorisation for den enkelte medarbejder.